IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for providing security for a computer network, comprising:

generating content sets for a computer associated with the network;

determining whether a user should be routed to the generated content sets;

selecting one of the content sets if it is determined that the user should be routed to the generated content sets; and

routing the user to a network interface associated with the selected generated content set;

wherein each generated content set is associated with one or more network interfaces associated only with that generated content set.

2. (Original) The method as recited in claim 1, further comprising monitoring the activities of the user with respect to the computer.

3. (Original) The method as recited in claim 2, further comprising preventing the user from accessing files associated with said monitoring.

4. (Original) The method as recited in claim 2, further comprising preventing the user from accessing processes associated with said monitoring.

5. (Original) The method as recited in claim 1, further comprising associating each generated content set with a virtual computer.

6. (Original) The method as recited in claim 5, wherein selecting one of the content sets includes choosing a content set associated with a virtual computer requested to be accessed by the user.

7. (Canceled)

8. (Currently amended) The method as recited in claim [[7]] 6, further comprising concealing from the user network interfaces not associated with the selected generated content set.

9. (Original) The method as recited in claim 5, further comprising concealing from the user network connections not associated with the selected generated content set.

10. (Original) The method as recited in claim 9, wherein concealing network connections includes receiving a request from the user to access a network connection, checking whether that network connection is associated with the selected generated content set, and if it is not associated with the selected generated content set, providing an indication that the network connection does not exist.

11. (Original) The method as recited in claim 9, wherein concealing network connections includes receiving a request from the user to access a network connection, checking whether that network connection is associated with the selected generated content set, and if it is not associated with the selected generated content set, transforming the request into a request to access a network connection associated with the selected generated content set.

12. (Original) The method as recited in claim 5, wherein the computer is running on a Unix operating system.

13. (Original) The method as recited in claim 12, wherein the computer is running on a Solaris operating system.

14. (Original) The method as recited in claim 1, wherein selecting one of the content sets includes choosing a content set associated with a service requested to be accessed by the user.

15. (Original) The method as recited in claim 14, wherein the service is telnet.

16. (Original) The method as recited in claim 1, wherein selecting one of the content sets includes choosing a content set not currently in use by another user.

17. (Original) The method as recited in claim 1, further comprising storing the packets sent by the user.

18. (Original) The method as recited in claim 1, further comprising logging information concerning the files to which the user requests access.

19. (Original) The method as recited in claim 1, further comprising preventing the user from accessing content within the computer other than the selected generated content set.

20. (Original) The method as recited in claim 1, further comprising screening a request by the user to access a file to determine if access is permitted.

21. (Original) The method as recited in claim 20, further comprising permitting access to a requested file if it is determined that access to the requested file is permitted.

22. (Original) The method as recited in claim 20, further comprising providing an indication that a requested file does not exist if it is determined that access is not permitted.

23. (Original) The method as recited in claim 1, further comprising generating additional content subsequent to the step of generating content sets.

24. (Original) The method as recited in claim 23, further comprising adding the additional content to the selected generated content set.

25. (Original) The method as recited in claim 1, wherein routing the user includes using network address translation to route to the selected generated content set any user who requests to access an unauthorized service.

26. (Original) The method as recited in claim 25, wherein the unauthorized service is telnet.

27. (Original) The method as recited in claim 1, further comprising receiving an indication that the user is no longer connected to the computer.

28. (Original) The method as recited in claim 27, further comprising determining whether to retain changes in the files of the computer that resulted from the user's activities.

29. (Original) The method as recited in claim 28, further comprising resetting the computer to restore the computer and the selected generated content set to the condition they were in prior to the user being routed to the selected generated content set if it is determined the changes should not be retained.

30. (Original) The method as recited in claim 29, further comprising updating the selected generated content set by generating additional content that appears to have been created during a time period during which the user was connected to the computer.

31. (Canceled)

32. (Canceled)

33. (Canceled)

34. (Canceled)

35. (Currently amended) A system for providing security for a computer network, comprising:

a computer configured to generate content sets for the computer, wherein the computer is associated with the network;

a plurality of network interfaces each associated with one of the content sets; and

a network device configured to determine whether a user should be routed to the generated content sets, select one of the generated content sets if it is determined that the user should be routed to the generated content, and to route the user to the selected generated content set;

wherein each generated content set is associated with one or more network interfaces associated only with that generated content set.

36. (Original) The system as recited in claim 35, wherein the network device is a firewall.

37. (Currently amended) A computer program product for providing security for a computer network, comprising a computer usable medium having machine readable code embodied therein for:

generating content sets for a computer associated with the network;

determining whether a user should be routed to the generated content sets;

selecting one of the generated content sets if it is determined that the user should be routed to the generated content sets; and

routing the user to a network interface associated with the selected generated content set;

wherein each generated content set is associated with one or more network interfaces associated only with that generated content set.

38. (Canceled)